IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Jürgen Büssert
Serial No.:	10/056,905
Date Filed:	November 13, 2001
Group Art Unit:	2131
Examiner:	Arani, Taghi T.
Title:	**ENCRYPTION OF CONTROL PROGRAMS**

MAIL STOP – APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPEAL BRIEF

Further to the notice of appeal submitted on March 19, 2007, Applicant hereby submits this appeal brief according to §41.37.

APPELLANT'S BRIEF (37 C.F.R. § 41.37)

This brief is submitted in support of appellants' notice of appeal from the decision dated February 7, 2007 of the Examiner finally rejecting claims 1-16 of the subject application.

I. REAL PARTY IN INTEREST

The real party in interest is:

Siemens AG
Wittelsbacherplatz 2
80333 München
GERMANY

by virtue of an assignment by the inventors as duly recorded in the Assignment Branch of the U.S. Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

The application as originally filed contained a total of 16 claims, in which Claims 1, 7, and 8 are independent. The status of the claims are as follows:

Claims Pending:	1-16
Claims Rejected:	1-16
Claims Allowed:	None
Claims Cancelled:	None
Claims Amended:	1, 5-8, 11-13, and 16
Claims Withdrawn:	None
Claims Objected:	None

Appellants appeal the rejection of claims 1-16 of the present application. These claims are reproduced in Appendix A.

IV. STATUS OF AMENDMENTS

Applicant amended Claims 1, 7 and 8 in a Response to Office Action filed on September 21, 2005. Claims 1, 5, 6, 8, 11, 12, 13, and 16 were further amended in a Response to Office Action filed August 1, 2006. No further claim amendments were submitted.

V. SUMMARY OF CLAIMED SUBJECT MATTER

CLAIM 1

Independent claim 1 is directed to "*A method for transferring control programs comprising:*

encrypting only a part of a control program code (5) in a first development system (1),"

See, specification, page 3, paragraph [0006]. Independent Claim 1 further comprises: "*transferring the encrypted control program code (10) from the first development system (1) to a second development system (3), and* "

See, specification, page 4, paragraph [0008] and paragraph [0009], lines 1-3. Independent Claim 1 further comprises: "*decrypting the encrypted control program code (16) in the second development system (3),*"

See, specification, page 5, paragraph [0011]. Independent Claim 1 further comprises:

" *wherein the decryption of the partially encrypted control program code (16) is carried out following editing (17) of the partially encrypted control program code (16) in the second development system (3).*"

See, specification, page 4, paragraph [0009], lines 7-8 and page 5, paragraph [0010].

CLAIM 8

Independent claim 8 is directed to "*A system for transferring control programs, comprising a first development device (1) for developing a control program code (5),*"

See, specification, page 3, paragraph [0005]. Independent Claim 1 further comprises: "*said first device (1) comprising an encryption unit (9) for encrypting only a part of the control program code(5),*" and

See, specification, page 3, paragraph [0006]. Independent Claim 1 further comprises: "*a communication device (14) for transferring the partially encrypted control program code (10) from the first development device (1) to a second development device (3),*"

See, specification, page 4, paragraph [0008] Independent Claim 1 further comprises: "*wherein said second development device (3) comprises an import device (15) for importing the partially encrypted control program code (16) and*"

See, specification, page 4, paragraph [0009], lines 1-3. Independent Claim 1 further comprises: "*an editor (17) for editing the control program (16) which is connected between a decryption device (18) for decrypting the partially encrypted control program code (16) and the communication device(15).*"

See, specification, page 4, paragraph [0009], lines 7-8 and page 5, paragraph [0010].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-16 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent 5,978,476 issued to Scott Redman et al. ("Redman") in view of U.S. Patent 6,904,527 issued to David B. Parlour et al. ("Parlour"). Applicant respectfully traverse and submit the cited art combinations, even if proper, which Applicant does not concede, does not render the claimed embodiment of the invention obvious.

VII. ARGUMENT

In the final office action dated October 18, 2006, the Examiner stated that *Redman* allegedly discloses all the limitations of independent Claims 1 and 8 except "encrypting a part of the control program code" and "decrypting the partially encrypted control program." (Final Office Action, dated Oct. 18, 2006, page 2, section 5 to page 3, second paragraph) Applicant respectfully disagrees.

In essence, the present independent Claims include the following steps (enumeration added and presented in chronological order):

(a) partially encrypting a program code in a first development system;

(b) transferring the partially encrypted program code to a second development system;

(c) editing the partially encrypted program code in the second development system;

(d) decrypting the edited partially encrypted program code.

Step (c) concerns the editing of a partially encrypted program code. This step is explained, for example, on page 4, paragraph [0009], lines 7-8 and page 5, paragraph [0010] of the specification. According to this description, only non-encrypted parts of the program code can be edited by a user. See, for example, page 5, paragraph [0010], lines 8-13. This makes sense because there would be nothing to edit in an encrypted code as the user would not know the meaning of the encrypted section.

Thus, contrary to the Examiner's conclusion and considering the above, *Redman* cannot disclose the step (c) because *Redman* discloses to completely encrypt the program code as correctly analyzed by the Examiner. Hence, there cannot be anything a user could edit unless he first decrypts the program code. A closer look to the specification of *Redman* cited by the Examiner (col. 7, line 55 through col. 8, line 17; See, Final Office Action, dated Oct. 18, 2006, page 3, second paragraph) which allegedly discloses step (c) reveals that *Redman* does not disclose this step. *Redman* states in the cited section:

> *"In the 'particular' embodiment of the invention discussed using Steps A to E in Section II, which uses DES encryption, operation of the design processing system 101 may be partially summarized in the following steps (which need not necessarily be taken in the order presented):*
>
> *Step P:* ***Accept*** *the authorization code from the user.*
>
> *Step Q:* ***Decrypt*** *the authorization code using a system DES key 307 (of FIG. 3) as the system decryption key 405 to obtain the permissions 117, including the vendor ID code and the product ID code; and maintain the permissions 117 within the system for use in handling subsequent requests from the user.*
>
> *Step R:* ***Accept*** *the user request 111.*
>
> *Step S:* ***Determine*** *from the permissions 117 whether the user has permission to have his request 111 be executed.*
>
> *Step T:* ***Reconstruct the design decryption key*** *305 according to Step B in Section II's discussion; i.e., by* ***modifying the "design encryption subkey"***

from the authorization code 115 by combining it with the vendor ID code and the product ID code.

*Step U: **Verify correctness of the design decryption key** 305 by recreating "Tag B" according to Step C in Section II's discussion, and confirming that the recreated Tag B is identical to the Tag B found in the header 211 of the encrypted design file 103.*

*Step W: **Use the verified design decryption key** 305 to decrypt the encrypted design file 103 into an internal representation of design information 411.*

Thereafter: Proceed to use design information 411 so long as the user has permission, as discussed above."

Redman, col. 7, line 60 to col. 8, line 22 (emphasis added). Steps P and R concerns the acceptance of the user request which hardly has anything to do with the "editing of program code." Step Q clearly concerns the decryption of a code which at best would be equal to step (d) and thus render all following steps of no concern when comparing them to the claim method steps. However, Step S also has nothing to do with "editing of program code." Moreover, steps T-W clearly concern the decryption key which is not part of the program code because it is used to decrypt the program code. Hence, *Redman* does not include the step of " *wherein the decryption of the partially encrypted control program code is carried out following editing of the partially encrypted control program code in the second development system.*"

Parlour does not add anything to *Redman* with this respect. Even if *Parlour* is interpreted to transmit an un-encrypted program code together with encrypted code, which Applicant does not concede, *Parlour* does not disclose the step of editing the un-encrypted code before the encrypted code is decrypted. Moreover, and most importantly, *Parlour* does not transfer program code from a first development system to a second development system for the purpose of editing the code in the second development system. The step of "editing program code" only makes sense in a development system. In automation systems, code is developed and adapted in development systems, such as engineering systems, and is then transferred to a runtime system where the code is executed. *Parlour* clearly discloses that the programmable logic device is not a second development system because *Parlour* actually

shows the second development system 104 in Fig. 2. The first development system 113 is operated by the vendor and designs the respective code and encrypts this code according to an encryption scheme. See, *Parlour,* col. 5, line 64 to col. 6, line 30. The code transmitted from the first development system 113 to the second development system 104 as described by *Parlour* is transmitted in its encoded form directly into the runtime system 102, namely the programmable logic device. Only within the runtime system 102 the code is decrypted. See, *Parlour*, col. 5, line 66 to col. 6, line 3.

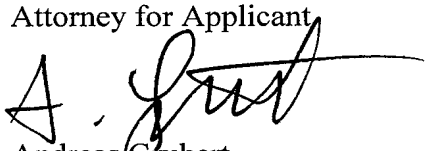
In summary, the cited prior art does not disclose the limitations of the present independent Claims. Applicant respectfully submits that the dependent Claims are allowable at least to the extent of the independent Claims to which they refer, respectively. Thus, Applicant respectfully requests reconsideration and allowance of the dependent Claims. Applicant reserves the right to make further arguments regarding the Examiner's rejections under 35 U.S.C. §103(a), if necessary, and do not concede that the Examiner's proposed combinations are proper.

SUMMARY

Applicant believes that the prior art cited do not render the independent claims obvious. Applicant respectfully submits that the dependent Claims are allowable at least to the extent of the independent Claim to which they refer, respectively. Thus, Applicant respectfully requests reconsideration and allowance of the dependent Claims.

Applicant hereby authorizes the Commissioner to charge the $500.00 filing fee, and any other fees necessary, or credit any overpayment, to Deposit Account No. 50-2148 of Baker Botts L.L.P.

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorney for Applicant



Andreas Grubert
Reg. No. 59,143

Date: May 16, 2007

SEND CORRESPONDENCE TO:
BAKER BOTTS L.L.P.
CUSTOMER ACCOUNT NO. **31625**
512.322.2545
512.322.8383 (fax)

VIII. CLAIMS APPENDIX

Claims:

1. (Previously Presented) A method for transferring control programs comprising

encrypting only a part of a control program code in a first development system,

transferring the encrypted control program code from the first development system to a second development system, and

decrypting the encrypted control program code in the second development system, wherein the decryption of the partially encrypted control program code is carried out following editing of the partially encrypted control program code in the second development system.

2. (Original) The method according to claim 1, further comprising exporting the encrypted control program code in a format that can be read by standard Internet clients via the first development system, and importing a data in the format that can be read by standard Internet clients via the second development system.

3. (Original) The method according to claim 1, wherein the encryption and decryption of the data is carried out by means of asymmetrical keys.

4. (Original) The method according to claim 1, wherein the encryption of the control program code is carried out following editing of the control program code in the first development system.

5. (Previously Presented) The method according to claim 1, wherein a head of the control program remains unencrypted.

6. (Previously Presented) The method according to claim 1, wherein the control program comprises a plurality of program modules and wherein different modules are encrypted differently.

7. (Previously Presented) A method for the configuration, project engineering and commissioning of a control system and a drive comprising transferring a control program according to claim 1, comprising compiling the decrypted control program, and processing the compiled control program by means of a microprocessor.

8. (Previously Presented) A system for transferring control programs, comprising a first development device for developing a control program code, said first device comprising an encryption unit for encrypting only a part of the control program code, , and a communication device for transferring the partially encrypted control program code from the first development device to a second development device, wherein said second development device comprises an import device for importing the partially encrypted control program code and an editor for editing the control program which is connected between a decryption device for decrypting the partially encrypted control program code and the communication device.

9. (Original) The system according to claim 8, wherein the first development device further comprises an export device for exporting the encrypted control program code in a format that can be read by standard Internet clients, and the second development device further comprises an import device for importing the data in the format that can be read by standard Internet clients.

10. (Original) The system according to claim 8, wherein the encryption and decryption of the data are carried out by means of asymmetrical keys.

11. (Previously Presented) The system according to claim 8, wherein the first development device further comprises a second editor for editing the control program code

and a communication device and a postprocessor for partially encrypting the control program code connected between said second editor and communication device.

12. (Previously Presented) The system according to claim 8, wherein the control program comprises a plurality of program modules and wherein different modules are encrypted differently.

13. (Previously Presented) The system according to claim 12, wherein different modules are encrypted with different encryption levels.

14. (Original) The system according to claim 8 utilized in an arrangement for the configuration, project engineering and commissioning of a control system and/or a drive.

15. (Original) A method according to claim 6, wherein a head part of the control program remains unencrypted.

16. (Previously Presented) The system according to claim 6, wherein different modules are encrypted with different encryption levels.

IX. EVIDENCE APPENDIX

NONE

X. RELATED PROCEEDINGS APPENDIX A

NONE